IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

JOSEPH CASEY, and RAQUEL AGEE, individually, and on behalf of all others similarly situated, Plaintiffs, vs. AT&T, INC., Defendant.	Case No. 3:24-cv-00803 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Joseph Casey ("Casey") and Raquel Agee ("Agee") (collectively "Plaintiffs"), individually, and on behalf of the class defined below, bring this class action complaint against AT&T, Inc., ("AT&T" or "Defendant") and allege as follows:

INTRODUCTION

1. Plaintiffs bring this action against AT&T for its failure to properly and adequately safeguard the personally identifying information ("PII") of tens of millions of current and former AT&T customers.

2. Defendant AT&T is a telecommunications provider headquartered in Dallas, Texas. AT&T provides consumer and business cellular, internet, and other telecommunications services throughout the United States. AT&T arose from the Bell Telephone Company, founded in 1877 by Alexander Graham Bell. Over the course of nearly one hundred and fifty years, and after a series of mergers and acquisitions in the telecommunication industry, AT&T has grown into the largest telecommunications company in the United States, with a market share of approximately 46% of wireless subscriptions.

3. As a requirement of providing services, AT&T collects critical PII from consumers, including, but not limited to, their names, email addresses, mailing addresses, birth dates, and Social Security Numbers.

4. On or about March 30, 2024, AT&T posted a notice on its website stating that "a number of AT&T passcodes have been compromised."[1] The notice further stated that "we will be communicating with current and former account holders with compromised sensitive personal information" but provided no specifics about what "sensitive personal information"

[1] *See* https://www.att.com/support/article/my-account/000101995?bypasscache=1, last visited April 1, 2024.

was involved (the "Data Breach").[2] AT&T confirmed that a "data set" consisting of data relating to 7.6 million current AT&T customers and approximately 65.4 million former account holders had been released on the dark web approximately two weeks prior.[3,4,5] AT&T further acknowledged that this "data set" included critical PII such as names, Social Security numbers, email addresses, mailing addresses, phone numbers, and birth dates.

5. News reports further indicate that this "data set" appears to relate to a data breach that occurred in 2021, but was never acknowledged or remedied in any way by AT&T.[6] *Id.* At least one news outlet reports that AT&T disputes this claim, yet the Company has failed to explain to Plaintiffs and Class Members who is responsible for the Data Breach and when it occurred.[7] Notably, in 2021, when data purported to be from this 2021 breach surfaced, AT&T denied that it had been breached. *Id.* Similarly, on March 22, 2024, when *TechCrunch* initially reported on the release of AT&T data on the dark web, AT&T stated "We have no indications of a compromise of our systems. We determined in 2021 that the information offered on this online forum did not appear to have come from our systems. This appears to be the same dataset that has been recycled several times on this forum." *Id.*

6. Plaintiffs seek to hold Defendant responsible for its failure to protect and keep

---

2 *Id.*

3 https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html, last visited April 1, 2024.

4 *See https://fortune.com/2024/03/31/att-data-breach-over-70-million-dark-web/*, last visited April 1, 2024.

5 https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web, last visited April 1, 2024.

6 https://techcrunch.com/2024/03/22/att-customers-data-leak-online/?guccounter=1 , last visited April 1, 2024.

7 https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web, last visited April 1, 2024.

secure the PII of Plaintiffs and similarly situated Class Members.

7. Plaintiffs further seek to hold Defendant responsible for its egregious failure to (a) identify the Data Breach, (b) identify its extent, and (c) promptly notify consumers.

8. At all relevant times, Defendant was aware of the risks of a Data Breach and that it would be specifically targeted by malicious hackers. Indeed, in 2021, AT&T competitor T-Mobile was the subject of a massive data breach involving the same critical PII, names, birth dates, and Social Security Numbers, that are at issue here.[8]

9. Armed with the PII from these records, hackers can sell the PII to other thieves or misuse the PII themselves to commit a variety of crimes that harm victims of the Data Breach. For instance, they can take out loans, mortgage property, open financial accounts, and open credit cards in a victim's name; use a victim's information to obtain government benefits; or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in another person's name; or give false information to police during an arrest.

10. As a result of Defendant's willful failure to prevent the Data Breach, Plaintiffs and Class Members are more susceptible to identity theft and have experienced, will continue to experience, and face an increased risk of financial harms, in that they are at substantial risk of identity theft, fraud, and other harm.

PARTIES

11. Plaintiff Joseph Casey is a resident of San Diego and a citizen of San Diego County, California. Plaintiff has been a wireless customer of AT&T for at least fifteen years. In order to receive services from AT&T, Plaintiff was required to provide PII such as his

[8] https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation, last visited April 1, 2024.

name, email address, mailing address, birth date, and Social Security Number. As a result of Defendant's actions, Plaintiff has been injured, has suffered financial losses, and will be subject to a substantial, continuing risk for further identity theft due to Defendant's Data Breach. Since learning of the Data Breach, Plaintiff has carefully monitored his financial accounts and credit reports. As a further result of Defendant's actions, Plaintiff will need to continue monitor his financial accounts and credit reports and take other measures to protect himself from identity theft and fraud. Plaintiff believed, at the time he opened a wireless account with AT&T, that AT&T would maintain the privacy and security of the PII he was required to provide. Plaintiff further believes he paid a premium to AT&T for its data security. Plaintiff would not have used AT&T had he known that it would expose sensitive customer PII, making it available to identity thieves.

12. Plaintiff Raquel Agee is a resident of Olivenhain and a citizen of San Diego County, California. Plaintiff was a customer of AT&T since approximately 2011, recently cancelling her services with Defendant. In order to receive services from AT&T, when she was an AT&T wireless customer, Plaintiff was required to provide PII such as her name, email address, mailing address, birth date, and Social Security Number. As a result of Defendant's actions, Plaintiff has been injured, has suffered financial losses, and will be subject to a substantial, continuing risk for further identity theft due to Defendant's Data Breach. Since learning of the Data Breach, Plaintiff has carefully monitored her financial accounts and credit reports. As a further result of Defendant's actions, Plaintiff will need to continue monitoring her financial accounts and credit reports and taking other measures to protect herself from identity theft and fraud. Plaintiff believed, at the time she opened a wireless account with AT&T, that AT&T would maintain the privacy and security of the PII she was required to

provide. Plaintiff further believes she paid a premium to AT&T for its data security. Plaintiff would not have used AT&T had she known that it would expose sensitive customer PII, making it available to identity thieves.

13. Defendant AT&T, Inc. is a Delaware corporation with its principal place of business located at 208 South Akard Street in Dallas, Texas. Defendant can be served through their registered agent CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). This lawsuit is a class action with an amount in controversy over $5 million, involving over 100 proposed class members, some of whom are from a different state than Defendant.

15. This Court may exercise personal jurisdiction over Defendant because Defendant is registered to do business and has its principal place of business in this district.

16. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

17. Defendant AT&T, Inc. is a Dallas, Texas-based telecommunications provider that provides, *inter alia*, cellular wireless services and internet services to consumers throughout the United States.

18. AT&T provides telecommunications, internet, or other services to more than

100 million U.S. consumers.[9] It is self-described as "the future of connectivity." *Id.*

19. In its Privacy Policy, AT&T represents that it will maintain the security and privacy of customers' personal information. For instance, AT&T states the following in its Privacy Policy:

> We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.[10]

20. AT&T also represents that, in the event of a data breach, it will notify impacted consumers:

> No security measures are perfect. We can't guarantee that your information will never be disclosed in a manner inconsistent with this notice. If a breach occurs, we'll notify you as required by law.[11]

21. The Privacy Policy also provides that Defendant collects a broad range of information on its customers including, *inter alia*:

- Name, postal address, email address, account name, Social Security number, driver's license number, passport number, taxpayer identification number, IP address, device IDs;
- Age, age range, date of birth, gender, preferred language, marital status;
- Biometric information such as Fingerprint, voiceprint, or scan of face geometry, that is used to identify a specific individual;
- Education information such as Degree(s), actual or inferred level of education;
- Professional or employment related information such as Current or past employment; history, licenses and professional membership.[12]

---

[9] https://investors.att.com/investor-profile#:~:text=AT%26T%20Communications%20provides%20more%20than,expansion%20and%20wireless%20network%20enhancements, last visited April 2, 2024.

[10] https://about.att.com/privacy/privacy-notice.html, last visited April 1, 2024.

[11] https://about.att.com/privacy/privacy-notice.html, last visited April 1, 2024.

[12] https://about.att.com/privacy/privacy-notice/state-disclosures.html#we-collect, last visited April 1, 2024.

22. On or about March 30, 2024, AT&T posted a notice on its website stating that "a number of AT&T passcodes have been compromised."[13] The notice further stated that "we will be communicating with current and former account holders with compromised sensitive personal information" but provided no specifics about the "sensitive personal information" involved in the Data Breach.[14] AT&T confirmed that, approximately two weeks prior to its announcement, the "data set," relating to 7.6 million current AT&T customers and approximately 65.4 million former account holders, had been released on the dark web.[15,16,17] AT&T further acknowledged that this "data set" included critical PII such as names, Social Security numbers, email addresses, mailing addresses, phone numbers, and birth dates.

23. News reports further indicate that this "data set" appears to relate to a data breach (the "Data Breach") that occurred in 2021, but was never acknowledged or remedied by AT&T.[18] At least one news outlet reports that AT&T disputes any connection to a 2021 Data Breach, however, the Company has identified neither who is responsible for the Data Breach nor when it occurred.[19] Notably, in 2021, when data purportedly from this 2021

[13] *See* https://www.att.com/support/article/my-account/000101995?bypasscache=1, last visited April 1, 2024.

[14] *Id.*

[15] https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html, last visited April 1, 2024.

[16] *See https://fortune.com/2024/03/31/att-data-breach-over-70-million-dark-web/*, last visited April 1, 2024.

[17] https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web, last visited April 1, 2024.

[18] https://techcrunch.com/2024/03/22/att-customers-data-leak-online/?guccounter=1 , last visited April 1, 2024.

[19] https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web, last visited April 1, 2024.

breach surfaced, AT&T denied that its customer data security had been breached.[20] Similarly, on March 22, 2024, when *TechCrunch* initially reported on the release of AT&T data on the dark web, AT&T stated, "We have no indications of a compromise of our systems. We determined in 2021 that the information offered on this online forum did not appear to have come from our systems. This appears to be the same dataset that has been recycled several times on this forum."[21]

24. AT&T's failure to protect the PII of current and former customers, and its failure to timely disclose the Data Breach, has left tens of millions of Class Members at heightened risk of financial fraud and identity theft.

B. AT&T is Well Aware of the Threat of Cyber Theft and Exfiltration in the Telecommunications Industry

25. As a condition of its relationships with its customers, including Plaintiffs and Class Members, Defendant required that they entrust it with highly sensitive and confidential PII. Defendant, in turn, collected that information and assured consumers that it was acting to protect that PII and to prevent its disclosure.

26. Plaintiffs and Class Members were required to provide their PII with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access and disclosure.

27. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on Defendant to keep their

[20] https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web, last visited April 1, 2024.

[21] *Id.*

PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

28. Defendant could have prevented the Data Breach by assuring that the PII at issue was properly secured.

29. Defendant's overt negligence in safeguarding Plaintiffs' and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as a business operating in the telecommunications space, Defendant was on notice that companies in that industry are targets for data breaches, especially in light of the massive 2021 data breach at competitor T-Mobile.

30. PII, including names and social security numbers are uniquely valuable to hackers. With these pieces of information, criminals can open new financial accounts in Class Members' names, take loans in their names, use their names to obtain medical services, obtain government benefits and/or identification, file fraudulent tax returns in order to get refunds to which they are not even entitled, and numerous other assorted acts of thievery and fraud.

31. Social Security numbers are among the most sensitive kind of personal information and the hardest to rehabilitate if it is misused or misappropriated. An individual cannot easily obtain a new Social Security number. Doing so, requires the completion of significant paperwork and provision of evidence of actual misuse. In other words, preventive action to guard against potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.

32. A new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to

link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

33. For this reason, hackers prey on companies that collect and maintain sensitive financial information, including telecommunications companies. Companies, like AT&T, have been aware of this, and the need to take adequate measures to secure their systems and customer information, for a number of years.

34. In 2021, 1,862 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, an increase of 68% over 2020 and a 23% increase over the previous all-time high. These data breaches exposed the sensitive data of approximately 294 million people. Id. Hackers are increasingly targeting highly sensitive PII, including social security numbers and, in 2021, approximately 1,136 data breaches exposed social security numbers.

35. Companies, like Defendant AT&T, are well aware of the risk that data breaches pose to consumers, especially because both the size of their customer base and the fact that the PII that they collect and maintain is profoundly valuable to hackers. Indeed, Federal Reserve Chairman Jerome Powell has referred to cyber-attacks as the number one threat to the global financial system.

36. It can be inferred from the Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs' and Class Members' PII.

37. Upon information and belief, prior to the Data Breach, Defendant was aware of its security failures but failed to correct them or to disclose them to the public, including Plaintiffs and Class Members.

38. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendant knew or should have known that it did not make such actions and failed to implement adequate data security practices.

39. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the PII of Plaintiffs and Class Members; and without the Court's intervention via injunctive relief, Representative Plaintiffs' and Class Members' PII remains at risk of subsequent data breaches.

40. Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and financial information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII financial information of Plaintiffs and Class Members.

41. Defendant owed a duty to Plaintiffs and Class Members to ensure that the PII it collected and was responsible for was adequately secured and protected.

42. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

43. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach that impacted the PII it collected and was responsible for in a timely manner.

44. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

45. Defendant owed a duty to Plaintiffs and Class Members to disclose if its data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

46. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

47. Defendant owed a duty to Plaintiffs and Class Members to mitigate the harm suffered by the Representative Plaintiffs' and Class Members' as a result of the Data Breach

48. As a direct and proximate result of Defendant's reckless and negligent actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, and Defendant's failure to properly and timely notify Plaintiffs and Class Members, Plaintiffs and Class Members are more susceptible to identity theft and have experienced, will continue to experience and will face an increased risk of experiencing the following injuries, *inter alia*:

a. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;

b. money and time lost as a result of fraudulent access to and use of their financial accounts;

c. loss of use of and access to their financial accounts and/or credit;

d. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;

e. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;

h. costs and lost time obtaining credit reports in order to monitor their credit records;

i. anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;

j. costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

k. money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;

l. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;

m. loss of the opportunity to control how their personal information is used; and

n. continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Defendant fails to undertake appropriate, legally required steps to protect the personal information in its possession.

C. AT&T's Inadequate Data Security Violated the FTC Act and the FCA

49. Pursuant to the Federal Trade Commission Act of 1915 ("FCTA"), AT&T was required to undertake reasonable and appropriate measures to protect the PII entrusted to it from unauthorized disclosure. Similarly, pursuant to the Federal Communications Act ("FCA"), common carriers, such as AT&T, are required to protect the consumer PII entrusted to it.

50. The Federal Trade Commission ("FTC") has adopted and published guidelines establishing reasonable and appropriate data security measures for businesses such as AT&T. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

51. The FTC has also published guidance titled, "Protecting Personal Information: A Guide for Business", which addresses steps that businesses should take to protect sensitive

consumer data, including noting that: "[i]f you don't have a legitimate business need for sensitive personally identifying information, don't keep it."[22] . Despite this guidance, AT&T appears to have kept a large amount of PII belonging to consumers who were no longer AT&T's customers. In addition, the FTC guide for business provides guidelines for maintaining network and data security, user authentication, breach detection, and other critical security best practices.[23] AT&T's failure to follow FTC guidelines, including, but not limited to, maintaining data on former customers, violated the guidelines. In addition, by its failure to adopt and maintain reasonable and adequate data security processes, AT&T engaged in unfair acts or practices within the meaning of the FTC Act.

CLASS ACTION ALLEGATIONS

52. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure 23(a), (b)(1), (2), (3), and (c)(4) on behalf of the classes defined as follows:

Nationwide Class: *All residents of the United States whose PII was accessed or otherwise compromised as a result of the Data Breach.*

California Subclass: *All residents of the state of California whose PII was accessed or otherwise compromised as a result of the Data Breach.*

Members of the Nationwide Class and the California Subclass are collectively referred to as "Class Members" and, unless stated otherwise, the Nationwide Class and California Subclass are referred to collectively as "the Class."

53. Excluded from the Class are Defendant, any entity in which Defendant has a

[22] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business, last visited April 2, 2024

[23] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business, last visited April 2, 2024.

controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

54. The proposed Nationwide Class and California Subclass meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (2),(3), and (c)(4).

55. **Numerosity:** Both the Nationwide Class and the California Subclass are so numerous that joinder of all members is impracticable. Based on information and belief, both the Nationwide Class and the California Subclass include millions of individuals who has their PII compromised, stolen, and published during the Data Breach. The parties will be able to identify the exact size of the class through discovery and AT&T's own documents.

56. **Commonality:** There are numerous questions of law and fact common to Plaintiffs and the Class including, but not limited to, the following:

- whether Defendant engaged in the wrongful conduct alleged herein;
- whether Defendant owed a duty to Plaintiffs and members of the Class to adequately protect their personal information;
- whether Defendant breached their duties to protect the personal information of Plaintiffs and Class members;
- whether Defendant knew or should have known that its data security systems, policies, procedures, and practices were vulnerable;
- whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's conduct, including increased risk of identity theft and loss of value of PII;
- whether Defendant violated state consumer protection statutes; and

- whether Plaintiffs and Class Members are entitled to equitable relief including injunctive relief.

57. **Typicality:** Plaintiffs' claims are typical of the claims of the Class members. Plaintiffs, like all Class members, had their personal information compromised in the Data Breach.

58. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no interests that are averse to, or in conflict with the Class Members. There are no claims or defenses that are unique to Plaintiffs. Likewise, Plaintiffs have retained counsel experienced in class action and complex litigation, including data breach litigation, and have sufficient resources to prosecute this action vigorously.

59. **Predominance:** The proposed action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Class predominate over any questions which may affect only individual Class Members.

60. **Superiority:** The proposed action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

61. Absent a class action, the majority of Class members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

62. **Risks of Prosecuting Separate Actions:** Plaintiffs' claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of separate

actions by individual class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendant. Defendant continues to maintain the PII of Class Members and other individuals, and varying adjudications could establish incompatible standards with respect to its duty to protect individuals' PII; and whether the injuries suffered by Class Members are legally cognizable, among others. Prosecution of separate actions by individual Class Members would also create a risk of individual adjudications that would be dispositive of the interests of other class members not parties to the individual adjudications, or substantially impair or impede the ability of Class Members to protect their interests.

63. **Injunctive Relief:** In addition, Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the class under Federal Rule of Civil Procedure 23(b)(2). Defendant continues to (1) maintain the PII of Class members, (2) fail to adequately protect said PII, and (3) violate Class Members' rights under state consumer protection laws and other claims alleged herein.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of the Nationwide Class against Defendant or, Alternatively, the California Subclass)

64. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

65. Plaintiffs bring this claim on behalf of themselves and the Class.

66. Plaintiffs and Class Members were required to provide Defendant with their PII. Defendant collected and stored this information including their names, Social Security numbers, email address, mailing address, birth date, and other PII.

67. Defendant had a duty to Plaintiffs and Class Members to safeguard and protect their PII.

68. Defendant assumed a duty of care to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

69. Defendant has full knowledge about the sensitivity of Plaintiffs' and Class Members' PII, as well as the type of harm that would occur if such PII was wrongfully disclosed.

70. Defendant has a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with user PII data.

71. Defendant breached their duty of care by failing to secure and safeguard the PII of Plaintiffs and Class members. Defendant negligently stored and/or maintained its data security systems and published that information on the Internet.

72. Further, Defendant by and through their above negligent actions and/or inactions, breached their duties to Plaintiffs and Class Members by failing to design, adopt, implement, control, manage, monitor, and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' PII within their possession, custody and control.

73. Plaintiffs and the other Class Members have suffered harm as a result of Defendant's negligence. These victims' loss of control over the compromised PII subjects

each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, or access to their user accounts.

74. It was reasonably foreseeable – in that Defendant knew or should have known – that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

75. But for Defendants' negligent and wrongful breach of their responsibilities and duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

76. As a direct and proximate result of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm for which they are entitled to compensation. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence/negligent misrepresentation.

77. Plaintiffs and Class Members are entitled to injunctive relief as well as actual and punitive damages.

SECOND CAUSE OF ACTION
Breach of Contract
(On Behalf of the Nationwide Class against Defendant or, Alternatively, the California Subclass)

78. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

79. Plaintiffs and Class Members entered into a contract with Defendant for the provision of title insurance or other closing services.

80. The terms of Defendant's privacy policy are part of the contract it enters with each Class Member to provide wireless services.

81. Plaintiffs and Class Members performed substantially all that was required of them under their contract with Defendant, or they were excused from doing so.

82. Defendant failed to perform its obligations under the contract, including by failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiffs and Class Member's information.

83. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received title insurance or other closing services that were less valuable than described in their contracts. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendant's deficient performance.

84. Also, as a result of Defendant's breach of contract, Plaintiffs and Class Members have suffered actual damages resulting from the exposure of their personal information, and they remain at imminent risk of suffering additional damages in the future.

85. Accordingly, Plaintiffs and Class Members have been injured by Defendant's breach of contract and are entitled to damages and/or restitution in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of the Nationwide Class against Defendant or, Alternatively, the California Subclass)

86. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

87. Defendant received a benefit from Plaintiffs and the Class in the form of payments for title insurance or other closing services.

88. The benefits received by Defendant were at the expense of Plaintiffs and Class Members.

89. The circumstances here are such that it would be unjust for Defendant to retain the portion of Plaintiffs' and Class Members' payments that should have been earmarked to provide adequate privacy, security, and confidentiality safeguards for Plaintiffs' and Class Members' personal information.

90. Plaintiffs and the Class seek disgorgement of Defendant's ill-gotten gains.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of the Nationwide Class against Defendant or, Alternatively, the California Subclass)

91. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

92. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of their use of Defendant's services. By providing their PII, and upon Defendant's acceptance of such information, Plaintiffs and Class Members, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contracts.

93. These implied-in-fact contracts obligated Defendant to take reasonable steps to secure and safeguard Plaintiffs' and Class Members' PII. The terms of these implied contracts are further described in the federal laws, state laws, and industry standards alleged above, and Defendant expressly assented to these terms in their Privacy Policy and other public statement described above.

94. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services, along with Defendant's promise to protect their PII from unauthorized disclosure.

95. In its Privacy Policy, Defendant expressly promised Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

96. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide PII was Defendant 's obligation to (a) use such PII for business purposes only; (b) take reasonable steps to safeguard that PII; (c) prevent unauthorized disclosures of the PII; (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses; and (f) retain the PII only under conditions that kept such information secure and confidential.

97. Without such implied contracts, Plaintiffs and Class Members would not have provided their PII to Defendant.

98. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

99. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII, which was compromised as a result of the Data Breach.

100. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure telecommunication services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives,

including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiffs and other Class Members have been put at an increased risk of identity theft, fraud, and/or misuse of their PII, which may take months if not years to manifest, discover, and detect.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of the Nationwide Class against Defendant or, Alternatively, the California Subclass)

101. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

102. In light of their special relationship, Defendant has become the guardian of Plaintiffs' and Class Members' PII and/ PHI. Defendant has become a fiduciary, created by its undertaking and guardianship of its customers' PII, to act primarily for the benefit of its customers, including Plaintiffs and Class Members. This duty included the obligation to safeguard Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

103. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to properly encrypt and otherwise protect the integrity of the system containing Plaintiffs' and Class Members' PII.

104. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) an increased risk of identity theft, fraud, and/or misuse of their PII; (c) the loss of the opportunity of how their PII is used; (d) the compromise, publication,

and/or theft of their PII; (e) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (f) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (g) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect customers' PII in their continued possession; and (h) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

105. As a direct and proximate result of Defendant's breach of their fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SIXTH CAUSE OF ACTION
BREACH OF IMPLIED COVENANT
OF GOOD FAITH AND FAIR DEALING
(On Behalf of the Nationwide Class or Alternatively, the California Subclass)

106. Plaintiffs, individually and on behalf of the Nationwide Class or alternatively the California Subclass, re-allege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

107. Plaintiffs and Class Members entered into valid, binding, and enforceable express or implied contracts with Defendant, as alleged above.

108. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their

contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the covenants that Defendant would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiffs' and Class Members' PII and to comply with industry standards and federal and state laws and regulations.

109. A "special relationship" exists between Defendant and the Plaintiffs and Class Members. Defendant entered into a "special relationship" with Plaintiffs and Class Members who entrusted Defendant, pursuant to Defendant's requirements, with their PII.

110. Despite this special relationship with Plaintiffs and Class Members, Defendant did not act in good faith and with fair dealing to protect Plaintiffs' and Class Members' PII.

111. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant.

112. Defendant's failure to act in good faith in implementing the security measures required by the contracts denied Plaintiffs and Class Members the full benefit of their bargain, and instead they received wireless and related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs and Class Members were damaged in an amount at least equal to this overpayment.

113. Defendant's failure to act in good faith in implementing the security measures required by the contracts also caused Plaintiffs and Class Members to suffer actual damages resulting from the theft of their PII, and Plaintiffs and Class Members remain at imminent risk of suffering additional damages in the future.

114. Accordingly, Plaintiffs and Class Members have been injured as a result of Defendant's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

SEVENTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of the California Subclass)

115. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

116. Plaintiffs bring this claim on behalf of themselves and the California Subclass.

117. Plaintiffs and California Subclass Members have a legally protected privacy interest in their PII that Defendant required them to provide and allow them to store.

118. Plaintiffs and California Subclass Members reasonably expected that their PII would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

119. Defendant unlawfully invaded the privacy rights of Plaintiffs and California Subclass Members by (a) failing to adequately secure their PII from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII to unauthorized parties without the informed and clear consent of Plaintiffs and Class members. This invasion into the privacy interest of Plaintiffs and California Subclass Members is serious and substantial.

120. In failing to adequately secure Plaintiffs' and California Subclass Members' PII, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiffs and California Subclass Members.

121. Defendant violated Plaintiffs' and California Subclass Members' right to privacy under the common law as well as under state and federal law, including, but not limited to, the California Constitution, Article I, Section I.

122. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiffs' and California Subclass Members' PII has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and California Subclass Members have suffered injury as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

EIGHTH CAUSE OF ACTION
Violation of California Consumers Legal Remedies Act, California Civil Code § 1750, *et seq.*
(On Behalf of the California Subclass against Defendant)

123. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

124. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq.* This cause of action does not seek monetary damages at this time but is limited solely to injunctive relief. Plaintiffs will later amend this Complaint to seek damages in accordance with the CLRA after providing Defendant with notice required by California Civil Code § 1782.

125. Plaintiffs and California Subclass Members are "consumers," as the term is defined by California Civil Code § 1761(d).

126. Plaintiffs, California Subclass Members, and Defendant has engaged in "transactions," as that term is defined by California Civil Code § 1761(e).

127. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the

conduct was undertaken by Defendant was likely to deceive consumers.

128. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

129. Defendant violated this provision by representing that they took appropriate measures to protect Plaintiffs and California Subclass Members' PII. Additionally, Defendant improperly handled, stored, or protected either unencrypted or partially encrypted data.

130. As a result, Plaintiffs and California Subclass Members were induced to enter into a relationship with Defendant and provide their PII.

131. As a result of engaging in such conduct, Defendant has violated Civil Code § 1770.

132. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiffs seek an order of this Court that includes, but is not limited to, an order enjoining Defendant from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

133. Plaintiffs and California Subclass Members suffered injuries caused by Defendant's misrepresentations, because they provided their PII believing that Defendant would adequately protect this information.

134. Plaintiffs and California Subclass Members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

135. The unfair and deceptive acts and practices of Defendant, as described above, present a serious threat to Plaintiffs and California Subclass Members.

NINTH CAUSE OF ACTION
Violation of Unfair Competition Law,
California Business and Professional Code Section 17200, *et seq*.
(On Behalf of the California Subclass against Defendant)

136. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

137. Plaintiffs brings this claim on behalf of themselves and California Subclass Members.

138. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

139. By reason of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs' and California Subclass Members' PII, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning of the UCL.

140. Defendant's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, in that the private and confidential PII of consumers has been compromised for all to see, use, or otherwise exploit.

141. Defendant's practices were unlawful and in violation of Civil Code § 1798 *et seq.* because Defendant failed to take reasonable measures to protect Plaintiffs' and California Subclass Members' PII.

142. Defendant's business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII they provide to Defendant will remain private and secure, when in fact it was not private and secure.

143. Plaintiffs and California Subclass Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendant's above-described wrongful actions, inactions, and omissions including, *inter alia*, the unauthorized release and disclosure of their PII.

144. Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and California Subclass Members' PII also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200 *et seq*., in that Defendant's conduct was substantially injurious to Plaintiffs and California Subclass Members, offensive to public policy, immoral, unethical, oppressive and unscrupulous; the gravity of Defendant's conduct outweighs any alleged benefits attributable to such conduct.

145. But for Defendant's misrepresentations and omissions, Plaintiffs and California Subclass Members would not have provided their PII to Defendant or would have insisted that their PII be more securely protected.

146. As a direct and proximate result of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and California Subclass Members' PII, they have been injured: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendant; (3) the compromise, publication, and/or theft of their PII; and (4) costs associated with monitoring their PII, amongst other things.

147. Plaintiffs takes upon themselves enforcement of the laws violated by Defendant in connection with the reckless and negligent disclosure of PII. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to

penalize Plaintiffs by forcing them to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

TENTH CAUSE OF ACTION
Violation of California Customer Records Act, California Civil Code § 1798.80 *et. seq*.
(On Behalf of the California Subclass against Defendant)

148. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

149. "[T]o ensure that personal information about California residents is protected," Civil Code section 1798.81.5 requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

150. Defendant owns, maintains, and licenses personal information, within the meaning of section 1798.81.5, about Plaintiffs and the California Subclass.

151. Defendant violated Civil Code section 1798.81.5 by failing to implement reasonable measures to protect Plaintiffs' and California Subclass Members' personal information.

152. As a direct and proximate result of Defendant's violations of section 1798.81.5 of the California Civil Code, the Data Breach described above occurred.

153. As a direct and proximate result of Defendant's violations of section 1798.81.5 of the California Civil Code, Plaintiffs and California Subclass Members suffered the damages described above including, but not limited to, time and expenses related to

monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personally identifying information.

154. Plaintiffs and California Subclass Members seek relief under section 1798.84 of the California Civil Code including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

ELEVENTH CAUSE OF ACTION
Injunctive/Declaratory Relief
(On Behalf of the Nationwide Class against Defendant or, Alternatively, the California Subclass)

155. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

156. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

157. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII they collected from Plaintiffs and Class Members.

158. Defendant owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure PII.

159. Defendant still possesses PII regarding Plaintiffs and Class Members.

160. Since the Data Breach, Defendant has announced few if any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

161. Defendant has not satisfied their contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

162. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

163. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

164. Plaintiffs therefore seek a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant not transmit PII via unencrypted email;

f. Ordering that Defendant not store PII in email accounts;

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

h. Ordering that Defendant conduct regular computer system scanning and security checks;

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request that the Court enter a judgment awarding the following relief:

a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Nationwide Class and California

Subclass requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class and California Subclass requested herein;

b. Declaratory relief requiring Defendant to (1) strengthen their data security systems that maintain personally identifying information to comply with the applicable state laws alleged herein and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendant's systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

c. An order requiring Defendant to pay all costs associated with class notice and administration of class-wide relief;

d. An award to Plaintiffs and all Class Members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

e. An award to Plaintiffs and all Class Members credit monitoring and identity theft protection services;

f. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

g. An order requiring Defendant to pay pre-judgment and post-judgment

interest, as provided by law or equity; and

h. Such other or further relief as the Court may allow.

Dated: April 3, 2024

Respectfully submitted,

By: */s/ Bruce W. Steckler*
STECKLER WAYNE & LOVE PLLC
BRUCE W. STECKLER
12720 Hillcrest Suite 1045
Dallas, Texas 75230
Telephone: (972) 387-4040
Cell: (214) 208-3327
bruce@stecklerlaw.com

BARRACK, RODOS & BACINE
STEPHEN R. BASSER
SAMUEL M. WARD*
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874
sbasser@barrack.com
sward@barrack.com

BARRACK, RODOS & BACINE
DANIELLE M. WEISS*
Two Commerce Square
2001 Market Street, Suite 3300
Philadelphia, PA 19103
Telephone: (215) 963-0600
dweiss@barrack.com

EMERSON FIRM, PLLC
JOHN G. EMERSON
2500 Wilcrest, Suite 300
Houston, TX 77042
Phone: 800-551-8649
Fax: 501-286-4659
jemerson@emersonfirm.com

Counsel for Plaintiffs Joseph Casey and Raquel Agee

*application for admission *Pro Hac Vice* forthcoming